KAJIAN YURIDIS DALAM ANTISIPASI KEJAHATAN CYBER

Jawade Hafidz
Email: jawade.hafidz@yahoo.com

Abstract

Cybercrime is one of the problems in Indonesia that its scope is derived from global international law. The rising rates of crime in the virtual world is influenced by factors of causality are difficult to obtain evidence by the action of the virtual world. When the Internet became accessible to everyone, they can do anything with the hunting of the target. For example, internet banking, hackers, search, can solve the data as amended rules become false data. cybercrime is a common problem that we have to finish up with serious legal rules.

In order to address the growing problem of cybercrime in Indonesia, the government makes laws and regulations specifically governing cyberlaw which were embodied as Act No. 11 of 2008 on Information and Electronic Transactions. Act No. 11 of 2008 as an effort to address cybercrime juridical and emperism, when Act No. 11 of 2008 not only addressed the issue of obscene or pornographic sites, but also establishes rules on electronic transactions is an umbrella rule of law in cyberlaw in Indonesia.

Keywords: *cyberlaw, cybercrime, cyberspace.*

Abstrak

Cybercrime merupakan salah satu masalah di Indonesia yang ruang lingkupnya berasal dari hukum global internasional. Peningkatan angka kejahatan di dunia maya dipengaruhi oleh faktor dari kausalitas yang sulit untuk mendapatkan bukti oleh aksi dunia maya. Ketika internet menjadi mudah diakses setiap orang, mereka dapat melakukan apa saja dengan berburu dari target. Misalnya, internet banking, hacker, pencarian, dapat memecahkan data aturan sebagaimana telah diubah menjadi data palsu. kejahatan siber merupakan masalah umum yang kita harus selesaikan dengan aturan hukum yang serius.

Dalam rangka mengatasi permasalahan cybercrime yang berkembang di Indonesia, pemerintah membuat aturan perundang-undangan yang khusus mengatur mengenai cyberlaw yang di wujudkan sebagai Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 11 Tahun 2008 merupakan salah satu upaya untuk mengatasi cybercrime secara yuridis dan emperism, padahal Undang-Undang Nomor 11 Tahun 2008 tidak hanya membahas masalah situs cabul atau pornografi, akan tetapi juga mengatur mengenai aturan-aturan tentang transaksi elektronik yang merupakan payung hukum dalam aturan cyberlaw di Indonesia.

Kata kunci : cyberlaw, cybercrime, cyberspace.

A. PENDAHULUAN

Perkembangan dunia informasi dan teknologi (IT) serta peningkatan jumlah para pengguna internet di Indonesia tidak dapat dipandang sebelah mata, rupanya semakin menguntungkan tiap orang untuk melakukan aktivitas tanpa batas *(borderless)*. Faktanya adalah tiap orang bisa mengakses segala hal informasi dengan canggih dan cepat.

Seiring kemajuan teknologi ternyata memunculkan masalah baru yaitu penyalahgunaan teknologi informasi untuk bertindak jahat atau yang sering disebut sebagai kejahatan cyber*(cybercrime)* yang dapat merugikan

orang lain. Yang lebih mengkhawatirkan ketika *cybercrime* merambah infrastruktur publik milik pemerintah maka dampaknya adalah kerugian nasional dan meresahkan masyarakat luas. *Cybercrime* adalah kejahatan konvensional yang modern. Karenanya hukum publik berupa jurisdiksi, etika kegiatan online, perlindungan konsumen, anti monopoli, persaingan sehat, perpajakan, regulatory body, data protection dan cybercrimes, dan hukum privat (HAKI, *E-commerce, Cyber Contract, Privacy, Domain name, Insurance*) menjadi kekuatan dasar negara untuk memerangi kejahatan tersebut.

Lahirnya hukum ITE *(Cyberlaw)* di negara kita disebabkan adanya aspek hukum yang dilakukan oleh subjek hukum yang memanfaatkan internet mulai pada saat "online" hingga memasuki dunia maya. Kemudian lahirlah hukum sistem informasi, hukum informasi, dan hukum telematika.

Jonathan Rosenoer (1997)[1] membagi ruang lingkup Cyberlaw dalam beberapa hal di antaranya: *Copy Right* (hak cipta), *Trademark* (hak merk), *Defamation* (pencemaran nama baik), *Hate Speech* (penistaan, penghinaan, fitnah), *Hacking, Viruses, Illegal Access*, (penyerangan terhadap komputer lain), *Regulation Internet Resource* (pengaturan sumber daya internet), *Privacy* (kenyamanan pribadi), *Duty Care* (kehati-hatian), *Criminal Liability* (kejahatan menggunakan IT), *Procedural Issues* (jurisdiksi, pembuktian, penyelidikan, dll.), *Electronic Contract* (transaksi elektronik), *Pornography*, *Robbery* (pencurian lewat internet), *Consumer Protection* (perlindungan konsumen), dan *E-Commerce, E-Government* (pemanfaatan internet dalam keseharian).

Darrel C Menthe berpendapat bahwa: *"The public interacts with cyberspace in two primary ways: either putting information into cyberspace or taking information out of cyberspace. At law in cyberspace, then, there are two distinct actors: the uploader and the downloader. Under this theory, the uploader and the downloader act like spies in the classic information drop the uploader puts information into a location in cyberspace, and the downloader accesses it at a later time. Neither need be aware of the other's identity"*[2]

Di samping itu, dalam Konggres PBB ke X di Wina, Austria pada tahun 2000, wacana cybercrime juga diisitilahkan lain dengan nama *computer related crimes* karena memiliki jangkauan akses tak terbatas yang luar biasa.

Secara teoritis, Menthe memberikan tiga gambaran teori mengenai karakteristik khusus yang terdapat dalam ruang cyberspace yaitu;

1. *The Theory of the Uploader and the Downloader*.
   Penafsiran daripada teori ini adalah suatu negara dapat melarang dalam wilayahnya, kegiatan *upload* dan *download* yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk uploading kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk downloading kegiatan perjudian tersebut.
   Minnesota adalah salah satu negara bagian pertama yang menggunakan jurisdiksi ini.[3]
2. *The Theory of Law of The Server.*
   Pendekatan ini memperlakukan server dimana webpages secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah webpages yang berlokasi di server pada Stanford University tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila uploader berada dalam jurisdiksi asing. Kesulitan terhadap bentuk kenyataan pengendalian server.

1 Rosenoer, Jonathan, 1997, "*Cyberlaw: The Law of Internet*", Springger, New York.

2 Masyarakat berinteraksi dengan dunia maya dalam dua cara utama: pertama, ia menempatkan informasi ke dunia maya atau mengambil informasi dari dunia maya. Pada hukum di dunia maya, maka, ada dua aktor yang berbeda: uploader dan downloader. Berdasarkan teori ini, para uploader dan downloader bertindak seperti mata-mata dalam informasi klasik drop-uploader menempatkan informasi ke lokasi di dunia maya, dan downloader mengakses itu di lain waktu. Meskipun menyadari identitas lain.

3 Lihat pada sumber http://fairuzelsaid.wordpress.com/2010/08/23/cyber-law-konsep-cyber-law/#more-2462, diakses Kamis, 21 Februari, pukul 22.10 WIB

3. *The Theory of International Spaces*. Ruang *cyberspace* dianggap sebagai *the fourth space*. Yang menjadi analogi adalah tidak terletak pada kesamaan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*.[4] Hukum untuk menangkap pelaku terbentur oleh teritori wilayah antar Negara.

Cyberlaw adalah peristilahan yang coba kita gagas apakah hal itu bisa kita terapkan kalau hanya merujuk pada Undang-Undang Nomor 11 tahun 2008 tentang Informasi danTransaksi Elektronik dan KUHP yang selama ini bisa dibuktikan relevansinya secara yuridis di Negara kita. Oleh sebab itu hemat penulis bahwa hukum adalah sanksi bagi para pelaku kejahatan apakah hukum tersebut harus melampaui wilayah terotorial sebuah Negara atau apakah hukum cyberlaw itu dapat dibuktikan berdasarkan aturan perundangan yang berlaku di Indonesia atau harus merujuk pada hukum *cyberlaw Internasional*.

Berdasarkan uraian tersebut, maka permasalahan yang perlu dikaji dalam Jurnal ini adalah bagaimana Kajian Yuridis Dalam Antisipasi Kejahatan Cyber ?

B. METODE PENELITIAN

Metode penelitian yang penulis gunakan sebagai pisau analisis adalah kwalitatif studi pustaka yang tentu diringi dengan beberapa kasuistiknya. Penekanan utama adalah bagiamana sumber teori penelitian mampu melahirkan suatu kesimpulan dengan latar penelitian kepustakaan (*Library Research*). Sasaran objek kajian penelitian ini menitikberatkan pada konsep pengertian *cyberlaw*, sejauh mana dampak *cybercrime* di Indonesia, serta peran hukum itu sendiri.

Kemudian arah penelitian mencoba menggali beberapa kesimpulan yang pasti, apakah ada penyimpangan pengertian terhadap para pelaku kejahatan yang beraksi di dunia internet yang bisa ditelisik secara hukum empiris berupa yuridis. Benarkah kekuatan hukum Negara kita yang betumpu pada KUHP dan UU ite Nomor 11 tahun 2008 dapat dijadikan sumber kekuatan hukum.

Teknik pengumpulan data berupa naskah data-data untuk melakukan analisis data krusial *cyberlaw, cybercrime*, dan *cyberspace*. Hal ini menekankan pada menggunakan perangkat tata bahasa sintaksis unng melingkupi wilayah dunia virtual tuk mengurai segala persoalan. Sehingga konsep melakukan koherensi dan relevansi penelitian akan menghasilkan suatu tinjauan pengertian yang sebenarnya dan mencapai kesepakatan antar beberapa teori dan kajian yang tepat.

Dalam penelitian hukum terdapat beberapa pendekatan, yaitu pendekatan undang-undang (*Statute Approach*), pendekatan kasus (*Case Approach*), pendekatan sejarah (*Historical Approach*), pendekatan komparatif (*Comparative Approach*), dan pendekatan konseptual (*Conceptual Approach*).[5]

Pendekatan perundang-undangan merupakan cara pendekatan dengan melihat peraturan perundang-undangan yang berkaitan dengan permasalahan yang dibahas. Penelitian untuk praktik hukum tidak dapat melepaskan diri dari pendekatan perundang-undangan. Pendekatan kasus sebagai komparasi hukum adalah digunakan apabila dalam membahas permasalahan menggunakan contoh kasus untuk mendapatkan gambaran yang jelas mengenai permasalahan yang dibahas.

C. HASIL DAN PEMBAHASAN

Dalam *Cyberspace* dunia itu adalah sempit sebab bisa dijangkau dengan singkat dan cepat. Rentannya pelanggaran yang seringkali diakibatkan oleh *Cyberspace* masyarakat awam berpendapat bahkan ada yang sengaja mentafsirkan sulit dijerat hukum karena hukum dan pengadilan di Negara Indonesia tidak mempunyai yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi melalui teknologi secara sahih.

Namun demikian kejahatan yang diakibatkan oleh peralatan teknologi adalah tetap disebut suatu pelanggaran hukum bersifat transnasional yang berdampak pada inplikasi hukum di Indonesia. Maka, setidaknya kita mengacu pada hukum internasional kalau kita menggagas betapa kekuatan hukum berupa Undang-Undang Informasi

4 Darrel C Menthe, 2004, *Jurisdiction in Cyberspace: A Theory of International Scraces, dalam http://www.mttlr.org/volfour/menthe.pdf, diakses pada Kamis 21 Februari 2013, pukul 22.00.*

5 Peter Mahmud Marzuki, 2005, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, hlm.93.

dan Transaksi Elektronik dan menyelaraskan KUHP. Dalam hukum internasional untuk menemukan yurisdiksi tentang *cyberlaw* terdapat tiga jenis yurisdiksi antara lain: yurisdiksi untuk menetapkan undang-undang *(the jurisdiction to prescribe)*, yurisdiksi untuk penegakan hukum *(the jurisdiction to enforce)*, dan yurisdiksi untuk menuntut *(the jurisdiction to adjudicate)*.[6]

Yurisdiksi adalah berlakunya hukum pidana menurut tempat yang sesungguhnya sudah tertera dalam KUHP yang didasarkan pada asas territorial, asas personal *(nasional aktif)* dan asas perlindungan *(nasional pasif)* serta asas universal.[7] Karena itu undang-undang khusus di luar KUHP tidak perlu membuat aturan tersendiri kecuali akan mengatur hal khusus yang belum diatur oleh KUHP.

Sementara kita melihat dasar Undang-Undang Telekomunikasi, Undang-Undang No. 36 Tahun 1999 Pasal 3, disebutkan bahwa "Telekomunikasi diselenggarakan dengan tujuan untuk mendukung persatuan dan kesatuan bangsa, meningkatkan kesejahteraan dan kemakmuran rakyat secara adil dan merata, mendukung kehidupan ekonomi dan kegiatan pemerintahan, serta meningkatkan hubungan antar bangsa".

Lahirnya Undang-Undang tersebut telah merubah sistem telekomunikasi di Indonesia yaitu: Telekomunikasi adalah salah satu infrastruktur penting dalam kehidupan berbangsa dan bernegara. Perkembangan teknologi yang sangat pesat tidak hanya terbatas pada lingkup telekomunikasi itu saja, malainkan sudah berkembang pada TI. Dan perkembangan teknologi telekomunikasi dituntut untuk mengikuti norma dan kebijaksanaan yang ada di Indonesia.[8]

Artinya bahwa locus itu bisa menjadi catatan hukum penting dalam menguak para pelaku *cybercrime* yang bergentayangan selama ini. *Locus delicate* menurut *Balck's Law Dictionary* adalah *the place where offense is commiteted: the place where the last event necessary to make the actor liable occurs*.[9] Bahwa *Locus delicate* merupakan tempat dimana suatu tindak pidana terjadi; suatu tempat dimana peristiwa kejadian (tindak pidana) dapat menyebabkan pelaku harus bertanggungjawab.

Persoalanya adalah apakah tindak pidana *cybercrime* tersebut terjadi di Indonesia atau bukan? Dan peradilan mana yang berhak dan berwenang untuk mengadili suatu perkara tersebut.

Oleh sebab itu, disinilah KUHP tentang pidana berperan sesuai dengan perumusannya seperti yang tertera dalam pasal 2-8 KUHP yaitu; apakah pelanggaran pidana tersebut terjadi di muka umum, pekarangan tertentu, atau ditempat yang biasa dilalui orang, atau diatas perahu Indonesia atau kapal Indonesia dan lain sebagainya.

Pandangan Utrecht, persoalan *locus delicate* dalam ilmu hukum pidana bersama dengan yurispundensi hukum pidana membuat tiga maacam teori yang bisa disebut sebagai kekuatan krusial untuk kita coba kupas perlakuan *cybercrime* yang semakin marak di Indonesia.[10]

Pertama, teori pembuatan materiil. Locus delicatenya adalah tempat dimana pembuat melakukan segala perbuatan yang dapat mengakibatkan delik yang bersangkutan. Karenanya *Locus delicate* adalah tempat dimana perbuatan yang perlu ada supaya delik dapat terjadi.

Kedua, teori alat yang dipergunakan. Delik dilakukan di tempat dimana alat yang dipergunakan itu menyelesaikannya. Dan *ketiga* adalah teori akibat. Disini *locus delicate* menjadi titik tekan dimana tempat akibat terjadinya.

Kemudian perkembangan *locus delicate* bisa kita lihat dari perbandingan yang dikatakan E.Y Kanter dan Sianturi, bahwa perkembangan pola pikir manusia mencetuskan *locus delicate* baru sebagai berikut: *pertama,* teori tindakan badaniah. Untuk menentukan tempat tindak pidana dibutuhkan teori tindakan badaniah dimana pelaku melakukan suatu tindak pidana, unsur-unsur tindak pidana pada saa itu bagaimana menjadi sempurna. *Kedua,* teori tempat bekerjanya alat. *Locus delicatenya* adalah dimana alat yang digunakan bekerja dan telah sempurna atau menimbulkan suatau tindakan pidana. *Ketiga,* teori akibat dari tindakan. Tempat tindak pidana adalah tempat terjadinya suatu akibat yang merupakan

6 Darrel C Menthe, 2004, *Jurisdiction in Cyberspace: A Theory of International Scracess*, (terj) Ahmad Ali, *Cyberlaw dan HAKI dalam sistem Hukum Indonesia*, Refika Aditama, Bandung, hlm.20

7 Lihat pada pasal 2, 5, 7, dan 8 dalam KUHP.

8 Lihat di sumber : http://www.tempo.co.id/hg/peraturan/2004/03/29/prn, 20040329-17,id.html, diakses pada Rabu 20 Februari 2013, pukul 09.00

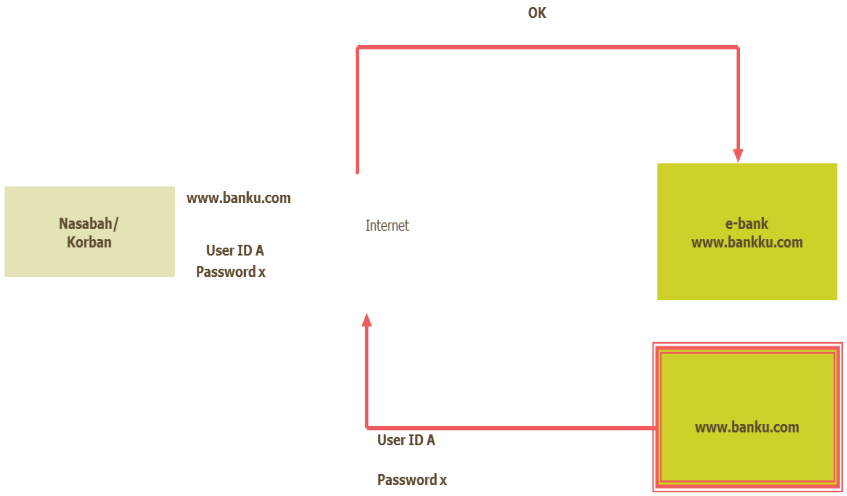
9 Bryan A. Garner,1999, *"Black's Law Dictionary seventh Edition",* St. Paul Minn: West Group, hlm.951

10 Utrecht, 1960, "*Hukum Pidana I"*, Penerbit Universitas Padjajaran Bandung.

penyempurnaan dari tindak pidana yang telah terjadi. *Keempat,* teori berbagai tempat tindak pidana. *Locus delicatenya* adalah gabungan ketiga-tiganya teori atau dua di antara ajaran-ajaran tersebut. Yakni gabungan antara beberapa teori berikut adalah teori perbuatan, teori alat yang digunakan, dan teori akibat.

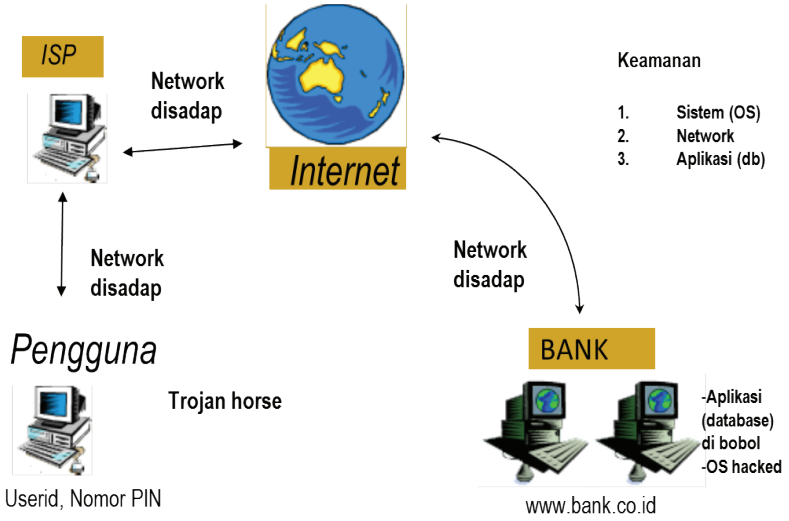
Disini penulis mencoba menyepakati apakah pendapat perkembangan locus delicate ini bisa menjadi perangkat untuk menelisik bentuk-bentuk tindak pidana dalam *cybercrime* yang semakin lama semakin berkembang. Sehingga tindak pidana itu tidak terjadi dalam satu tempat saja melainkan di beberapa tempat seperti yang kerap terjadi dalam perlakuan *cybercrime* lebih lanjut. Kasus *typosit* (situs palsu) misalnya, *locus delicate* dalam mencari yurisdis untuk melangkah ke tahap pidana selanjutnya dan untuk mendapatkan pelaku dimana dia berada, di tempat mana dia melakukan kejahatan tersebut. Kinerja kejahatan tersebut kalau kita kerangkakan dari berbagai sumber maka bisa kita lihat pada bagan di bawah ini:

Gb.1. Kerja dan tempat untuk melakukan kejahatan Typosit (situs palsu)



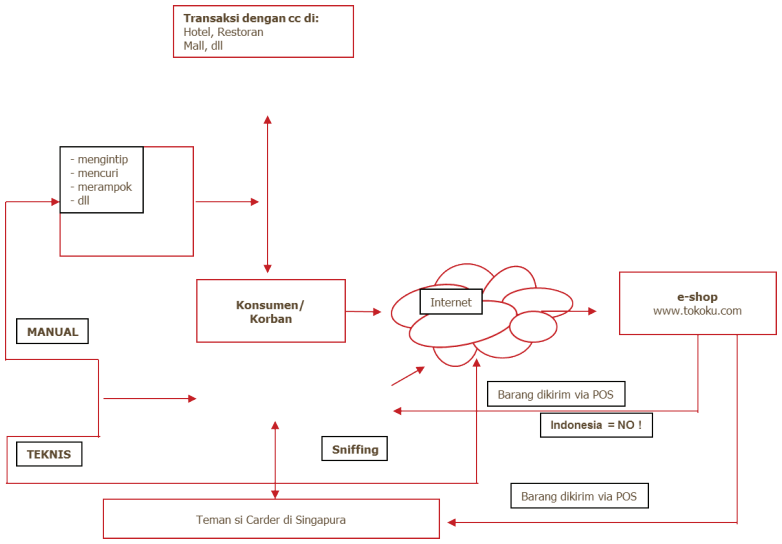
Sedangkan kalau kita mau melihat beberapa contoh kasus lain seperti kejahatan cybercrime yang sering dilakukan melalu jejaring sosial lain seperti *key-longger, E-banking,* dan *carding* sebagai berikut;

Gb. 2. *Kerja dan tempat untuk melakukan kejahatan E-banking*

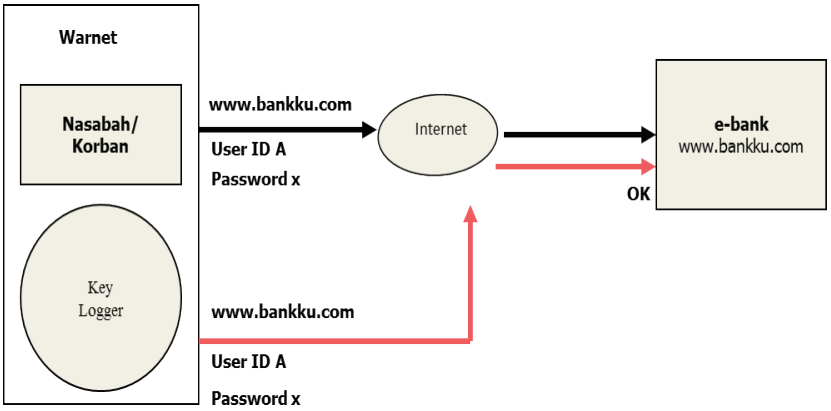


11 *Ibid.*

Gb.3. Kerja dan tempat untuk melakukan kejahatan *Carding*



Gb.4. Kerja dan tempat untuk melakukan kejahatan *Key-Longger*



Cybercrime dengan jalan demikian kerap terjadi dan jarang bisa ditemukan *locus delicatenya*. Peran hukum untuk menemukan tindak pidana diperlukan upaya penguatan konstruksi hukum yang sejalan dengan hukum internasional.

Kalau kita mengacu pada Undang-Undang ITE (Informasi Dan Transaksi Elektronik) Nomor 11 Tahun 2008 Presiden Republik Indonesia sebagai berikut:

Menimbang :

a. *Bahwa pembangunan nasional adalah salah satu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika di masyarakat.*
b. *Bahwa globalisasi informasi telah menempatkan indonesia sebagai bagian dari masyarakat informasi dan transaksi elektronik di tingkat nasional seentuk hingga pembangunan teknologi informasi dapat dilakukan secara optimal,merata,dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.*
c. *Bahwa perkembangan dan kemajuan teknologi informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru.*
d. *Bahwa penggunaan dan pemanfaatan teknologi informasi harus terus dikembangkan untuk menjaga,memelihara,dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional.*

e. *Bahwa pemanfaatan teknologi informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat.*
f. *Bahwa pemerintah perlu mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturanya sehingga pemanfaatan teknologi informasi memperhatikan nilai-nilai agama dan sosial budaya masyarakat indonesia.*
g. *Bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f, perlu membentuk undang-undang tentang informasi dan transaksi elektronik.*

Dan akhirnya Presiden Republik Indonesia dan Dewan Perwakilan Rakyat (DPR) telah memutuskan menetapkan, Undang-undang tentang Informasi Transaksi Elektronik pada tahun 2008 sebagai berikut:

I. Bab I, tentang Ketentuan Umum
II. Bab II, tentang Asas dan Tujuan
III. Bab III, tentang informasi, dokumen, dan tanda tangan elektronik
IV. Bab IV, tentang penyelenggaran dan sertifikasi elektronik dan sistem elektronik
V. Bab V, tentang transaksi elektronik
VI. Bab VI, tentang domain hak kekayaan intelektual,dan perlindungan hak pribadi
VII. Bab VII, tentang perbuatan yang dilarang
VIII. Bab VIII, tentang penyelesain sengketa
IX. Bab IX, tentang peran pemersyaraintah dan masyarakat
X. Bab X, tentang penyidikan
XI. Bab XI, tentang ketentuan pidana
XII. Bab XII,tentang ketentuan peralihan
XIII. Bab XIII, tentang ketentuan penutup

Persoalan hukum dalam mencari yurisdis untuk menindak *Cybercrime* adalah bagian dari upaya hukum untuk menguatkan kesepakatan dan sanksi hukum yang telah diputuskan pemerintah pada tahun 2008, sebagaimana Undang-Undang Informasi dan Transaksi Elektronik yang kita gunakan sekarang untuk menjerat para pelaku *Cybercrime* di Indonesia. Namun persoalan *cyberlaw* tersebut bersifat transnasional-internasional.

Relevansi dari hukum tersebut apakah menjadikan Undang-Undang Informasi dan Transaksi Elektronik itu sudah bisa dijadikan alat hukum yang kuat dalam menemukan locus delicatenya yang mencakup yurisdis hukum dalam menangangi merebaknya kejahatan melalui dunia virtual atau penyelewengan terhadap fungsi internet tersebut?

Bahwa merebaknya kejahatan yang dilakukan lewat jejaring sosial memang tidak bisa disamakan dengan kejahatan pada umumnya. Kejahatan tersebut cukup sulit dalam tahap penyelesaian nya sebab kejahatan Informasi dan Transaksi Elektronik adalah kejahatan tingkat modern yang syarat dengan kecanggihan sistem komunikasi yang membutuhkan kecerdasan seperangkat teknologi.

Untuk memaksimalkan hukum tersebut agar tetap berjalan berdasarkan strandart etik dan hukum maka diperlukan dua hal. *Pertama,* adalah prinsip hukum. Pemerintah, swasta dan professional adalah unsur keterlibatan utama dalam memantau perkembangan teknologi di Indonesia. Kerjasama dalam memerangi *cybercrime* antara pemerintah, swasta dan professional bukan hanya menjadi sinergitas melainkan upaya dan kewajiban bersama dalam rangka melindungi negara dari kejahatan yang dilakukan secara modern.

Kedua, melakukan tinjauan hukum perundangan nasional yang terkait langsung maupun tidak langsung akibat munculnya persoalan yang ditimbulkan oleh perkembangan transaksi melalui teknologi-internet. Misalnya; Undang-Undang Hak Cipta, Undang-Undang Hak Merk, Undang-Undang Penyiaran, Undang-Undang Informasi dan Komunikasi, Undang-Undang Kontrak, Undang-Undang Perseroan Terbatas, Undang-Undang pidana, Undang-Undang Pajak, Undang-Undang Penanaman Modal Asing dan sebagainya, terkontrol kontinu setiap ada kasus yang diakibatkan oleh *cybercrime.*

Lantas perlindungan terhadap penyalahgunaan internet dan komputer diperlukan tinjauan dan pembentukan hukum modern. Artinya melakukan modernisasi hukum material dan acara pidana

tidak semata-mata berbasis pencegahan. Tapi revitalisasi hukum modern adalah kewajiban bagi pemerintah. Sehingga perlindungan terhadap korban *cybercrime* memenuhi kebijakan.

Bagi para hakim, pejabat, dan aparat penegak hukum tentang *cybercrime* selain peningkatan kualitas dan saling bekerja sama, mereka harus mempertajam pengetahuan analisis motodis yang seyogyanya menjadi kekuatan dasar untuk terciptanya produk hukum modern di Negara ini dalam rangka memerangi kejahatan di dunia teknologi.

"Dunia *cyber* secara metodis tidak terpatri pada kaidah umum yang kebanyakan orang mengatakan tidak bisa ditanggulangi. Cyber berasal dari kata *"Cybernetics"* yang bertujuan untuk mengendalikan sesuatu dari jarak jauh seperti robot yang bisa dikontrol dari jarak jauh".

Jadi dunia *cyber* tujuannya adalah untuk mengendalian sistem total. Karena itu sangat tidak mungkin jika dunia cyber tersebut tidak bisa dikendalikan kalau kita berkaca pada fungsi dan tujuannya.

Kita bisa ambil contoh yang pernah terjadi di Indonesia *typosite* (situs palsu) seperti gambar di atas. Nasabah sengaja dipancing untuk melakukan kesalahan ketik alamat masuk ke situs tersebut. Jenis kejahatan ini tidak jauh beda dengan memanfaatkan kelemahan sistem layanan *online banking*. Kalau hal itu merambah ke seluruh sendi-sendi saluran informasi dan teknologi di beberapa perusahaan besar negara ini, berapa besar kerugian nasional yang akan terjadi.

Berapa jumlah penduduk yang kecewa dan resah akibat mandulnya hukum dan proteksi keamanan IT di Negara kita sehingga menimbulkan kemacetan transaksi nasional yang melibatkan pemerintah dan masyarakat. Karena itu Undang-Undang Informasi dan Transaksi Elektronik memberikan kepastian hukum tentang bentuk-bentuk transaksi elektronik yang dapat dijadikan alat bukti sah. Selama ini bentuk-bentuk transaksi elektronik yang hanya dibuktikan sebagai selembar kertas bukti transfer misalnya tidak bisa dijadikan alat bukti karena memang belum ada payung hukumnya untuk itu.[11]

11 Lihat di sumber http://nasional.kompas.com/read/2008/03/25/20464694/polisi .Berharap.Ada.UU.Cyber.Crime, diakses pada Kamis 21 Februari 2013, pukul 22.15 WIB.

D. PENUTUP

1. KESIMPULAN

Payung hukum Negara kita untuk mengantisipasi *cybercrime* adalah Undang-Undang Informasi dan Transaksi Elektronik yang dipersepsikan sebagai *cyberlaw* hingga mampu menjadi harapan untuk dapat mengatur rotasi kegiatan dan segala urusan dunia teknologi dan internet termasuk di dalamnya memberi *punishment* terhadap pelaku *cybercrime*. Mengingat bahwa *cybercrime* bisa kita simpulkan sebagai kejahatan yang menggunakan Teknologi Informasi Sebagai Fasilitas: Pembajakan, Pornografi, Pemalsuan/ Pencurian Kartu Kredit, Penipuan Lewat Email (*Fraud*), Email Spam, Perjudian *Online*, Pencurian *Account Internet*, Terorisme, Isu Sara, Situs Yang Menyesatkan, dan sebagainya.

Terkadang *cybercrime* cukup menyulitkan yurisdiksi hukum tapi bukan berarti tidak bisa ditangani ketika bukti itu ada. Alasan sulitnya adalah; pertama, kegiatan dunia cyber tidak dibatasi oleh teritorial Negara, Kedua, Kegiatan dunia cyber relatif tidak berwujud hingga secara hukum tradisional kadang sulit untuk menemukan bukti yang dapat disebut pembuktian karena data elektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan ke seluruh belahan dunia dalam hitungan detik.

Demikian juga dengan apabila ada kejahatan dunia maya, pencurian *bandwidth, carding, typosit*, dan sebagainya apakah memungkinkan menghadirkan alat bukti dalam konteks *cyberspace. Hardware* hanya alat yang belum tentu bisa menjamin kepastian yurisdis dan ketetapan bukti hukum yang pasti.

2. SARAN

Berdasarkan pada beberapa temuan di atas penulis bermaksud bahwa hukum sebagai pondasi tegaknya suatu keadilan perlu peremajaan manakala hukum konvensional atau tradisional tak lagi mampu menjadi kekuatan ayat

atau pasal dalam menangkap tindak kriminalitas melalui dunia maya. Hal ini mengingatkan pada diri penulis dan bagi para pengguna internet di Indonesia setidaknya sadar bahwa maraknya kejahatan virtual yang diakibatkan kenakalan objek melalui cyberspace adalah bentuk pelanggaran terhadap Undang-Undang Informasi dan Transaksi Elektronik Republik Indonesia Nomor 11 tahun 2008 dan berimbas pada kerugian atau dapat merugikan masyarakat luas. Dalam pandangan hukum baik KUHP maupun pembuktian secara yurisdis ketika dapat diwujudkan maka hal itu tetap mendapatkan sanksi pidana seperti kasus-kasus yang pernah terjadi di Indonesia, Asia dan Internasional.

DAFTAR PUSTAKA

- **Buku-Buku**

Budi Raharjo, 2004, *"Keamanan Sistem Informasi Berbasis Internet",* Handbook Keamanan, Jakarta, PT Insan Indonesia-Bandung & PT. Indocisc.

Bryan A Garner, 1999, *"Black's Law Dictionary seventh Edition",* ST. Paul Minn: West Gro up.

Darrel C Menthe, 2004, *"Jurisdiction in Cyberspace: A Theory of International Scracess",* (terj) Ahmad Ali, *Cyberlaw dan HAKI dalam sistem Hukum Indonesia*, Bandung, Refika Aditama.

Peter Mahmud Marzuki, 2005, *"Penelitian Hukum",* Jakarta, Kencana Prenada Media Group.

Raharjo, Budi, 2002, *"Memahami Teknologi Informasi",* Jakarta, Elexmedia Komputindo.

Rosenoer, Jonathan, 1997, *"Cyberlaw: The Law of Internet",* New York, Springger.

Utrecht, 1960, *"Hukum Pidana I",* Bandung, Penerbit Universitas Padjajaran.

- **Peraturan Perundang-Undangan:**

Undang-Undang Republik Indonesia tentang ITE (Informasi Dan Transaksi Elektronik) Nomor 11 Tahun 2008

Undang-Undang KUHP Pasal 2, 5, 7, dan 8.

- **Internet**

http://www.tempo.co.id/hg/peraturan/2004/03/29/prn,20040329-17,id.html, diakses pada Rabu 20 Februari 2013, pukul 09.00 WIB.

http://www.mttlr.org/volfour/menthe.pdf, diakses pada Kamis 21 Februari 2013, pukul 22.00 WIB.

http://fairuzelsaid.wordpress.com/2010/08/23/cyber-law-konsep-cyber-law/#more-2462, diakses Kamis, 21 Februari, pukul 22.10 WIB.

http://cyberlaw.wordpress.com/2007/08/11/menjerat-pelaku-cyber-crime-dengan kuhp/, diakses pada Rabu 20 Februari 2013, pukul 09.15 WIB.

http://nasional.kompas.com/read/2008/03/25/20464694/Kepolisian.Berharap.Ada.UU.Cyber.Crime, diakses pada Kamis 21 Februari 2013, pukul 22.15 WIB.